This document is scheduled to be published in the Federal Register on 08/31/2021 and available online at **federalregister.gov/d/2021-18710**, and on **govinfo.gov**

4334-

DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2019-0006; 201D0102DM, DS65100000, DLSN00000.000000, DX65103]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, Interior.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) proposes to modify the DOI-50, Insider Threat Program, system of records. The DOI Office of Law Enforcement and Security uses this system to identify potential threats to DOI resources and information assets and facilitate management of insider threat investigations, complaints, inquiries, and counterintelligence threat detection activities. DOI is publishing this revised system of records notice to reflect the updated system location and system manager address, authorities, expand the scope of categories of individuals and categories of records in the modified system, propose new and modified routine uses, and provide general and administrative updates to the remaining sections of the notice. Additionally, DOI is publishing a Notice of Proposed Rulemaking elsewhere in the *Federal Register* to exempt this system of records from certain provisions of the Privacy Act. This modified system will be included in DOI's inventory of record systems.

DATES: This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].** Submit comments on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by docket number [DOI-2019-0006], by any of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for sending comments.
- Email*:* DOI_Privacy@ios.doi.gov. Include docket number [DOI-2019-0006] in the subject line of the message.
- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2019-0006]. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240, DOI_Privacy@ios.doi.gov or (202) 208-1605.

SUPPLEMENTARY INFORMATION:

I. Background

The DOI Office of Law and Enforcement and Security (OLES) maintains the Insider Threat Program system of records. This system of records helps the OLES manage insider threat matters and counterintelligence threat detection and prevention within the DOI. The Insider Threat Program was mandated by Presidential Executive Order 13587, issued October 7, 2011, which requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. The OLES uses this system to detect, deter and mitigate potential threats to the DOI resources and information assets; facilitate insider threat investigations, complaints, and inquiries; and conduct counterintelligence threat detection activities.

Insider threats include attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against the DOI and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into proprietary information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary-information or technology; and indicators of potential insider threats or other

incidents that may indicate activities of an insider threat. This system may include information from any DOI bureau, office, program, record or source, and includes records from information security, personnel security, and systems security for both internal and external security threats.

The DOI is publishing this revised notice to update authorities, reflect the expanded scope of categories of records and categories of individuals covered by the modified system, add a new section to describe the purpose of the system, and provide general and administrative updates to the remaining sections of the notice in accordance with the Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. Additionally, the DOI is modifying existing routine uses to further provide clarity and transparency, and reflect updates consistent with standard DOI routine uses. The DOI is proposing new routine uses to facilitate the sharing of information with agencies and organizations as necessary to ensure the efficient and effective management of inquiries, investigations, or referrals related to insider threat or counterintelligence matters, promote the integrity of the records in the system, or carry out a statutory responsibility of the DOI or Federal Government.

Routine uses A, B, H, I, and O have been modified to provide additional clarification on external organizations and circumstances where disclosures are proper and necessary to facilitate insider threat investigations or comply with Federal requirements. Modified routine use J and new routine use K allow the DOI to share information with appropriate Federal agencies or entities when reasonably necessary to respond to a breach of personally identifiable information and to prevent, minimize, or remedy the risk of harm to individuals or the Federal Government, or assist an agency in locating individuals affected by a breach in accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Proposed routine use N allows sharing with the news media and the public, when it is necessary to preserve the confidence in the integrity of the DOI, demonstrate the accountability of its officers, employees, or individuals covered in the system, or where there exists a legitimate public interest in the disclosure of the information such as circumstances that support a legitimate law enforcement or public safety function, or protects the public from imminent threat of life or property. Proposed routine use R allows DOI to share information with third parties when necessary to obtain information pertinent to an investigation. Proposed routine use S allows DOI to share information with a public or professional licensing organization when there is an indication of potential violation of professional standards. Proposed routine use T facilitates sharing with other Federal agencies in support of authorized counterintelligence activities. Proposed routine use U allows DOI to share information with any individual, organization or entity to notify them of a serious threat to homeland security so they may guard against or respond to the threat when relevant to the protection of life, health or property. Proposed routine use V allows sharing of information with the House Committee on Oversight and Government Reform and the Senate Homeland Security and Governmental Affairs Committee pursuant to a written request made under 5 U.S.C. 2954. Proposed routine use W allows DOI to share information with Federal agencies or entities regarding counterintelligence or insider threat matters, to obtain information or guidance on the handling of the matter. Proposed routine use X allows DOI to share information with former DOI employees, contractors or individuals who were sponsored by DOI for security clearance to respond to official inquiries or to facilitate communications or obtain information that is relevant and necessary for personnel related purposes or other official purpose as required by DOI. Proposed routine use Y facilitates sharing of records for audit and oversight purposes as authorized by law and where necessary and proper to the audit or oversight function. Proposed routine use Z allows

DOI to share information with prospective or current employers to determine employment eligibility.

In a Notice of Proposed Rulemaking, which is published separately in the *Federal Register*, the DOI is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(5).

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of the DOI by complying with DOI Privacy Act regulations at 43 CFR part 2, Subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the *Federal Register* a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. The revised DOI-50, Insider Threat Program, system of records notice is published in its entirety below. In accordance with 5 U.S.C. 552a(r), the DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Participation

You should be aware that your entire comment including your personally

identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER:

INTERIOR/DOI-50, Insider Threat Program.

SECURITY CLASSIFICATION:

Classified and unclassified.

SYSTEM LOCATION:

Counterintelligence Unit, Office of Law Enforcement and Security, U.S. Department of the Interior, 12201 Sunrise Valley Drive, Reston, VA 20192.

SYSTEM MANAGER(S):

DOI Counterintelligence/Insider Threat Program Manager, Counterintelligence Unit, Office of Law Enforcement and Security, U.S. Department of the Interior, 12201 Sunrise Valley Drive, Reston, VA 20192.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458; Intelligence Authorization Act for FY 2010, Public Law 111-259; Title 28 U.S.C. 535, Investigation of Crimes Involving Government Officers and Employees; Limitations; Title 50 U.S.C. 402a, Coordination of Counterintelligence Activities; Executive Order 10450, Security Requirements for Government Employment, April 17, 1953; Executive Order 12333, United States Intelligence Activities (as amended); Executive Order 12829, National Industrial Security Program; Executive Order 12968, Access to Classified Information, August 2, 1995; Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and

Eligibility for Access to Classified National Security Information, June 30, 2008; Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009; Executive Order 13526, Classified National Security Information; Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011; Presidential Memorandum National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012; and Security Executive Agent Directives issued by the Office of the Director of National Intelligence.

PURPOSE(S) OF THE SYSTEM:

The purposes of the Insider Threat Program system of records are to manage counterintelligence and insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence complaints, inquiries and investigations; identify potential threats to DOI resources and information assets; evaluate and track DOI employees on foreign travel; evaluate and track foreign visitors as part of the Foreign Visitors Program; review and evaluate individuals and companies desiring to conduct business with DOI; evaluate and track supply chain risks; track referrals of potential insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered in the system include current and former DOI employees, potential employees, and contractors; other officials or employees of Federal, state, tribal, territorial, and local law enforcement organizations; complainants, informants, suspects and witnesses; covered individuals who have been granted access to controlled unclassified information or classified information, or who hold a sensitive

position; persons requesting or having access to DOI facilities, information systems, programs, and infrastructure; members of the general public, including individuals and/or groups of individuals who report or are involved with counterintelligence or insider threat matters, complaints or incidents involving classified information or systems, or controlled unclassified information; individuals being investigated as potential insider threats; individuals desiring to conduct business with DOI; individuals involved in contracts, bids, or proposals related to procurement or acquisition activities; individuals identified as the result of an administrative, security or investigative function who could pose a threat to DOI operations, data, personnel, facilities and systems; family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation; and foreign visitors or foreign contacts that become involved in potential counterintelligence or insider threat matters.

This system maintains records on U.S. citizens, non-U.S. citizens and foreign nationals; however, the Privacy Act only applies to individuals who are U.S. citizens or aliens lawfully admitted for permanent residence.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system maintains records related to counterintelligence activities and referrals or investigations of potential insider threats. Records include incident reports; criminal, civil or administrative investigative records; background investigations; personnel security records; facility access records; network security and communications records; information systems security logs; analyses and reports; security violations, and inquiries and recommended remedial actions related to suspected security violations; official and foreign travel records; foreign visitor records; records of contacts with foreign persons; financial disclosure reports; financial records; personnel records; medical records; criminal history records; drug test results; training records; information on complainants, informants, suspects, and witnesses; information from Standard Form

(SF) 85 and SF 86 questionnaires; Closed Circuit Television (CCTV) recordings; polygraph examination records; document control registries; courier authorization requests; derivative classification unique identifiers; requests for access to sensitive compartmented information (SCI); briefing/debriefing statements for special programs, sensitive positions, and related information required in connection to personnel security clearance determinations; results of preliminary screening reviews; exhibits, evidence, statements, and affidavits; permits or leases related to DOI infrastructure or managed resources; bids, contracts, procurements or acquisition activities related to individuals and organizations desiring to conduct business with DOI; and other records involving potential insider threats or activities directed against DOI and its personnel, facilities, systems or resources.

These records may contain: name, Social Security number, date of birth, place of birth, citizenship, security clearance, home address, work address, personal or official phone number, personal or official email address, other contact information, drivers license number, vehicle identification number, license plate number, ethnicity and race, tribal identification number or other tribal enrollment data, work history, educational history, affiliations, information on family members, dependents, relatives and other personal associations, passport number, gender, fingerprint, hair and eye color, photographic image, video recording, voiceprint, biometric data, any other physical or distinguishing attributes of an individual, and publicly available social media account information.

Investigation records and incident reports may include additional information such as photos, video, sketches, medical reports, and network use records, identification badge data, facility and access control records, email and text messages. Records may also include information concerning potential counterintelligence or insider threat activity, counterintelligence complaints, investigative referrals, results of incident

investigations, case number, forms, nondisclosure agreements, consent forms, documents, reports, investigative or analytical efforts of DOI Insider Threat Program personnel, intelligence reports and database query results relating to individuals covered by this system; information obtained from other Federal agencies, organizations, or sources about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat, including but not limited to espionage or unauthorized disclosures of controlled unclassified information and classified national security information; and correspondence, documents and reports received, generated or maintained in the course of managing insider threat activities and conducting investigations related to the protection of DOI resources and information assets against potential insider threats.

RECORD SOURCE CATEGORIES:

Sources of information in the system include Department, bureau, office and program officials, employees, contractors, and other individuals who are associated with or represent the DOI; officials from other Federal, Tribal, State, territorial, and local government organizations; other Federal agencies, organizations, or sources providing information about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat, including but not limited to espionage or unauthorized disclosures of classified national security information or controlled unclassified information; relevant DOI records, databases and files, including personnel security files, facility access records, security incidents or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports; and complainants, informants, suspects, and witnesses.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the U.S. Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) DOI or any component of DOI;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any DOI employee or former employee acting in his or her official capacity;

(4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The U.S. Government or any agency thereof, when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office in response to a written inquiry that an individual covered by the system has made to the office, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j) and (k).

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j) and (k).

D. To any criminal, civil, or regulatory law enforcement authority (whether

Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records;

(2) DOI has determined that as a result of the suspected or confirmed breach there

is a risk of harm to individuals, DOI (including its information systems, programs, and operations), the Federal government, or national security; and

(3) the disclosure made to such agencies, entities and persons is reasonably necessary to assist in connection with DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(1) responding to a suspected or confirmed breach; or

(2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

O. To the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, the Office of the Director of National Intelligence, and other Federal, State, territorial and local law enforcement agencies for the purpose of referring potential counterintelligence or insider threats and information exchange on

counterintelligence and or insider threat activity.

P. To agency contractors, grantees, or volunteers for DOI or other Federal Departments who have been engaged to assist the Government in the performance of a contract, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity.

Q. To any criminal, civil, or regulatory authority (whether Federal, State, territorial, local, or tribal) for the purpose of providing background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

R. To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the individual making the disclosure.

S. To a public or professional licensing organization for the purpose of verifying information, or when information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

T. To any Federal, State, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations lawfully engaged in intelligence or counterintelligence activities, national security, homeland defense, counterterrorism, or law enforcement intelligence for that entity's official responsibilities, including responsibilities to counter, deter, prevent, prepare for, respond to, threats to national or homeland security, including an act of terrorism or espionage.

U. To any individual, organization, or entity, as appropriate, to notify them of a

serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or when there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.

V. To members of the House Committee on Oversight and Government Reform and the Senate Homeland Security and Governmental Affairs Committee pursuant to a written request under 5 U.S.C. 2954, or other committee with oversight of matters within their jurisdiction pertaining to Insider Threat Program activities, after consultation with the Senior Agency Official for Privacy and legal counsel.

W. To a Federal agency or entity that has information relevant to an allegation or investigation regarding an insider threat for purposes of obtaining guidance, additional information, or advice from such federal agency or entity regarding the handling of a counterintelligence or insider threat matter, or to a federal agency or entity that was consulted during the processing of the allegation or investigation but that did not ultimately have relevant information.

X. To a former DOI employee, DOI contractor, or individual sponsored by DOI for a security clearance for purposes of responding to an official inquiry by Federal, State, local, tribal, or territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be relevant and necessary for personnel-related or other official purposes when DOI requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Y. To an agency or organization for the purpose of performing audits or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

Z. To an individual’s prospective or current employer to the extent necessary to

determine employment eligibility.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic records are maintained in information systems, or stored on magnetic disc, tape or digital media. Paper records are maintained in file cabinets in a secure facility behind a locked door.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name, Social Security number, date of birth, phone number, and other types of information by keyword search.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A records retention schedule for the Insider Threat Program has been developed and submitted to NARA for approval. Pending approval by NARA, these records will be treated as permanent. The proposed records disposition is temporary. Records in the Insider Threat Program system of records related to a particular insider threat will be maintained for twenty-five years from the date when the insider threat was discovered. Records related to cases that are not insider threats will be destroyed three years after notifications of death, or five years after (1) the individual no longer has an active security clearance held by DOI, (2) separation or transfer of employment, or (3) the individual's contract relationship with DOI expires; whichever is applicable. Approved disposition methods include shredding or pulping paper records, and degaussing or erasing electronic records in accordance with 384 Department Manual 1 and NARA guidelines.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. During normal hours of operation, paper records are maintained in locked file cabinets under the control of

authorized personnel. Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974 (Pub. L. 93–579), Paperwork Reduction Act of 1995 (Pub. L. 104–13), Federal Information Security Modernization Act of 2014 (Pub. L. 113–283), and the Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. Computer servers in which electronic records are stored are located in secured Department of the Interior facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Security controls include encryption, firewalls, audit logs, and network system security monitoring.

Electronic data is protected through user identification, passwords, database permissions and software controls. Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

RECORD ACCESS PROCEDURES:

The Department of the Interior has exempted portions of this system from the access procedures of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5). An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

The Department of the Interior has exempted portions of this system from the amendment procedures of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5). An individual requesting correction or the removal of material from his or her records should send a signed, written request to the System Manager identified above. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

The Department of the Interior has exempted portions of this system from the notification procedures of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5). An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system contains classified and unclassified intelligence and law enforcement investigatory records related to insider threat and counterintelligence activities that are exempt from certain provisions of the Privacy Act, 5 U.S.C. 552a(j) and (k). Pursuant to 5 U.S.C. § 552a(j)(2), (k)(1), (k)(2) and (k)(5), the Department of the Interior has exempted portions of this system from the Privacy Act subsections (c)(3), (c)(4), (d), (e)(1) through (e)(3), (e)(4)(G) through (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), and (g). In accordance with 5 U.S.C. 553(b), (c) and (e), the Department of the Interior has promulgated rules at 43 CFR part 2, subpart K, and is proposing to amend these rules in a Notice of Proposed Rulemaking published separately in the *Federal Register*.

HISTORY:

79 FR 52033 (September 2, 2014).

Teri Barnett,

Departmental Privacy Officer,
Department of the Interior.
[FR Doc. 2021-18710 Filed: 8/30/2021 8:45 am; Publication Date: 8/31/2021]